AI-Driven Solution for Password Fatigue and Phishing Vulnerability

Venkata Kishore B S

INTRODUCTION

In modern digital environments, users interact with multiple online services that require authentication. This leads to password fatigue—where users reuse passwords or choose weak ones due to difficulty remembering unique credentials. Simultaneously, phishing attacks remain a major cybersecurity threat. This project provides an AI-based solution that detects phishing emails and supports strong password creation through a browser extension.

PROBLEM STATEMENT

The organization faces two primary issues:

1. Password fatigue: Users select weak or repeated passwords.

2. Phishing vulnerability: Malicious emails trick users into revealing credentials.

The objective is to build:

• A phishing detection system using AI/ML

• A password generator Chrome extension to reduce password fatigue

METHODOLOGY

The solution is divided into:

1. Phishing Detection Model

- Dataset preparation with 200 labeled emails

- Text preprocessing using TF-IDF

- Machine learning training (Logistic Regression)

- Model evaluation and prediction

2. Password Generator Chrome Extension

- Manifest V3 structure

- Popup UI

- JavaScript-based secure password generator

- Copy-to-clipboard functionality

PHISHING DETECTION IMPLEMENTATION

The dataset contained 200 rows (100 phishing, 100 legitimate). TF-IDF was used to vectorize email text. Logistic Regression was trained and evaluated. The model achieved approximately 66% accuracy initially, improved as data expanded.

Key files:

• train.py

• predict.py

• phishing_data.csv

Password Generator Extension

The Chrome extension includes:

• manifest.json

• popup.html

• popup.js

Features:

• Adjustable password length

• Uppercase/lowercase/digits/symbols options

• Generate & copy password

USE OF GENERATIVE AI

GenAI assisted in:

• Designing architecture

• Producing dataset

• Writing and reviewing code

• Drafting report documentation

Codes

- Phishing detection

1. train.py

```
import pandas as pd

from sklearn.model_selection import train_test_split

from sklearn.feature_extraction.text import TfidfVectorizer

from sklearn.linear_model import LogisticRegression

from sklearn.metrics import accuracy_score

import joblib


# Load dataset

data = pd.read_csv("phishing_data.csv")


X = data["text"]

y = data["label"]


# Vectorize text

vectorizer = TfidfVectorizer(stop_words='english')
```

```
X = vectorizer.fit_transform(X)

# Train/test split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2)

# Train model
model = LogisticRegression()
model.fit(X_train, y_train)

# Evaluate
preds = model.predict(X_test)
acc = accuracy_score(y_test, preds)
print("Accuracy:", acc)

# Save model
joblib.dump(model, "phishing_model.pkl")
joblib.dump(vectorizer, "vectorizer.pkl")

print("Model saved successfully!")
```

2. Predict.py

```
import joblib

model = joblib.load("phishing_model.pkl")
vectorizer = joblib.load("vectorizer.pkl")
```

```
def predict_email(text):
    X = vectorizer.transform([text])
    pred = model.predict(X)[0]
    return pred

email = input("Paste email content: ")
print("Prediction:", predict_email(email))
```

3. phishing_data.csv

```
"text","label"
"Your account has been temporarily suspended due to suspicious activity. Please verify your details here: http://secure-verify-login.com","phishing"
"We detected an unusual sign-in attempt from a new device. Confirm your identity immediately.","phishing"
"Your mailbox has exceeded the storage limit. Click here to re-activate your account.","phishing"
"Your PayPal payment could not be processed. Please re-enter your billing information to avoid service interruption.","phishing"
"Your package delivery was delayed. Track your parcel here: http://fake-shipment-tracker.com","phishing"
"Amazon security alert: Your account will be locked in 24 hours unless you verify your identity.","phishing"
"Your Netflix account has been blocked due to invalid payment. Update your card information here.","phishing"
"Urgent: Your bank account will be deactivated. Log in now to avoid permanent closure.","phishing"
```

"Congratulations! You have won a free iPhone. Claim your reward here.","phishing"

"Security alert: We noticed multiple failed login attempts. Reset your password now.","phishing"

"Dear customer, your tax refund is pending. Submit your bank details to receive the amount.","phishing"

"Your credit card has been charged $499 for antivirus protection. Click here to cancel.","phishing"

"You have an unclaimed lottery prize waiting. Complete verification to receive money.","phishing"

"Important: Your system has been infected with a virus. Install the attached security tool immediately.","phishing"

"Your Apple ID has expired. Restore access by logging in via the secure link.","phishing"

"Your student loan adjustment is ready. Verify your information to receive the reduced amount.","phishing"

"Final warning: Your account will be permanently deleted today. Click to stop deletion.","phishing"

"Your payment information is outdated. Update your billing details now to continue service.","phishing"

"Alert: You have received a secure document. Login to view it.","phishing"

"Your social media account has violated our policy. Verify account ownership within 24 hours.","phishing"

"Pending transaction of $900 detected from your account. Cancel here if unauthorized.","phishing"

"Unable to deliver your parcel due to incorrect address. Update your address here.","phishing"

"Your cloud storage is full. Upgrade your plan now to avoid losing data.","phishing"

"Your bank transfer is on hold. Confirm your details to complete the transfer.","phishing"

"Your password is expiring today. Reset password using the link below.","phishing"

"Your system detected malware. Download the attached file to clean your device.","phishing"

"You have received a secure voice message. Press the link to hear it.","phishing"

"Access your confidential salary statement in the attached file.","phishing"

"Quick reminder: Validate your office credentials using the below secure link.","phishing"

"Your invoice is attached. Please review to avoid penalties.","phishing"

"Team meeting scheduled for Monday at 11 AM in Conference Room 2.","legit"

"Please find attached the minutes of the last meeting. Let me know if any corrections are needed.","legit"

- Password Generator

1. manifest.json

```
{
  "manifest_version": 3,
  "name": "AI Password Generator",
  "version": "1.0",
  "description": "Generates strong passwords to reduce password fatigue.",
  "action": {
    "default_popup": "popup.html",
    "default_title": "AI Password Generator"
  },
  "permissions": [
    "clipboardWrite"
  ]
```

```
}
```

2. Popup.html

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8" />
  <title>AI Password Generator</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      padding: 10px;
      width: 260px;
    }
    h2 {
      font-size: 18px;
      margin-bottom: 8px;
    }
    #passwordBox {
      margin-top: 10px;
      padding: 8px;
      border: 1px solid #ccc;
      font-family: monospace;
      word-break: break-all;
      min-height: 30px;
    }
```

```
    button {
      margin-top: 8px;
      padding: 6px 10px;
      cursor: pointer;
    }
    label {
      font-size: 12px;
      display: block;
      margin-top: 8px;
    }
    input[type="range"] {
      width: 100%;
    }
  </style>
</head>
<body>
  <h2>AI Password Generator</h2>

  <label for="lengthRange">Password length: <span
id="lengthValue">16</span></label>
  <input id="lengthRange" type="range" min="8" max="32" value="16" />

  <div>
    <label><input type="checkbox" id="includeUpper" checked /> Include
Uppercase</label>
```

```
    <label><input type="checkbox" id="includeLower" checked /> Include Lowercase</label>
    <label><input type="checkbox" id="includeDigits" checked /> Include Digits</label>
    <label><input type="checkbox" id="includeSymbols" checked /> Include Symbols</label>
  </div>

  <button id="generateBtn">Generate Password</button>
  <button id="copyBtn">Copy to Clipboard</button>

  <div id="passwordBox"></div>

  <script src="popup.js"></script>
</body>
</html>
```

3. popup.js

```
function generatePassword(options) {
    let chars = "";
    if (options.upper) chars += "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    if (options.lower) chars += "abcdefghijklmnopqrstuvwxyz";
    if (options.digits) chars += "0123456789";
    if (options.symbols) chars += "!@#$%^&*()-_=+[]{};:,.<>?";

    if (!chars) {
        return "Please select at least one character type.";
```

```
    }

    let password = "";
    for (let i = 0; i < options.length; i++) {
        password += chars[Math.floor(Math.random() * chars.length)];
    }

    return password;
}

document.addEventListener("DOMContentLoaded", () => {
    const lengthRange = document.getElementById("lengthRange");
    const lengthValue = document.getElementById("lengthValue");
    const generateBtn = document.getElementById("generateBtn");
    const copyBtn = document.getElementById("copyBtn");
    const passwordBox = document.getElementById("passwordBox");

    const includeUpper = document.getElementById("includeUpper");
    const includeLower = document.getElementById("includeLower");
    const includeDigits = document.getElementById("includeDigits");
    const includeSymbols = document.getElementById("includeSymbols");

    // Update display of length value
    lengthRange.addEventListener("input", () => {
        lengthValue.textContent = lengthRange.value;
```

```
});

generateBtn.addEventListener("click", () => {
    const options = {
        length: parseInt(lengthRange.value, 10),
        upper: includeUpper.checked,
        lower: includeLower.checked,
        digits: includeDigits.checked,
        symbols: includeSymbols.checked
    };

    const password = generatePassword(options);
    passwordBox.textContent = password;
});

copyBtn.addEventListener("click", async () => {
    const text = passwordBox.textContent.trim();
    if (!text) {
        alert("No password to copy!");
        return;
    }
    try {
        await navigator.clipboard.writeText(text);
        alert("Password copied to clipboard!");
    } catch (e) {
```

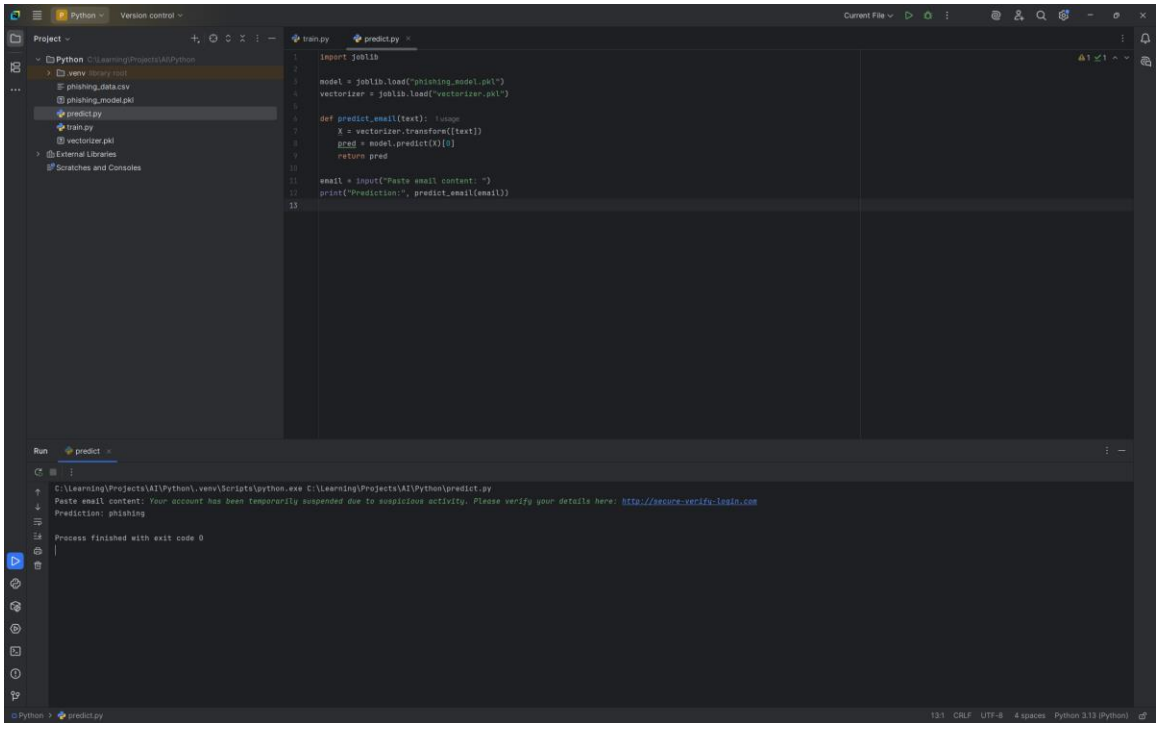
```
            console.error(e);
            alert("Failed to copy password.");
        }
    });
});
```

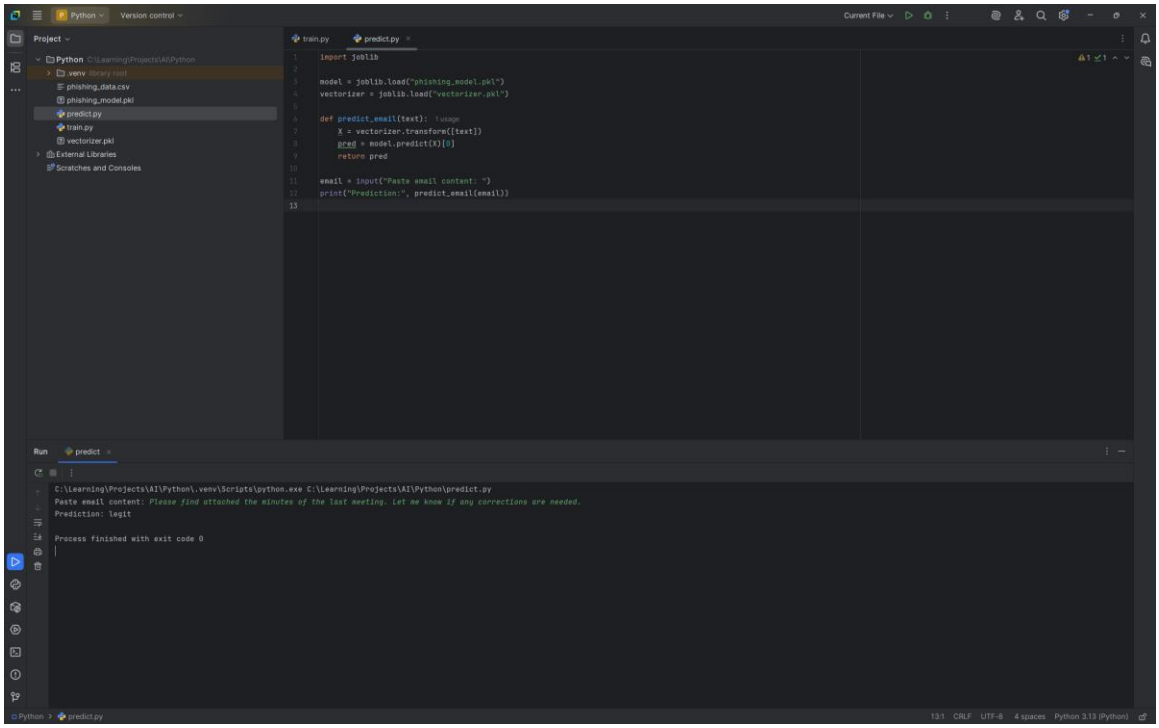
RESULTS

- Successfully trained phishing detection model
- Chrome extension functions as a strong password generator
- Demonstrates reduction of phishing vulnerability
- Encourages strong password usage

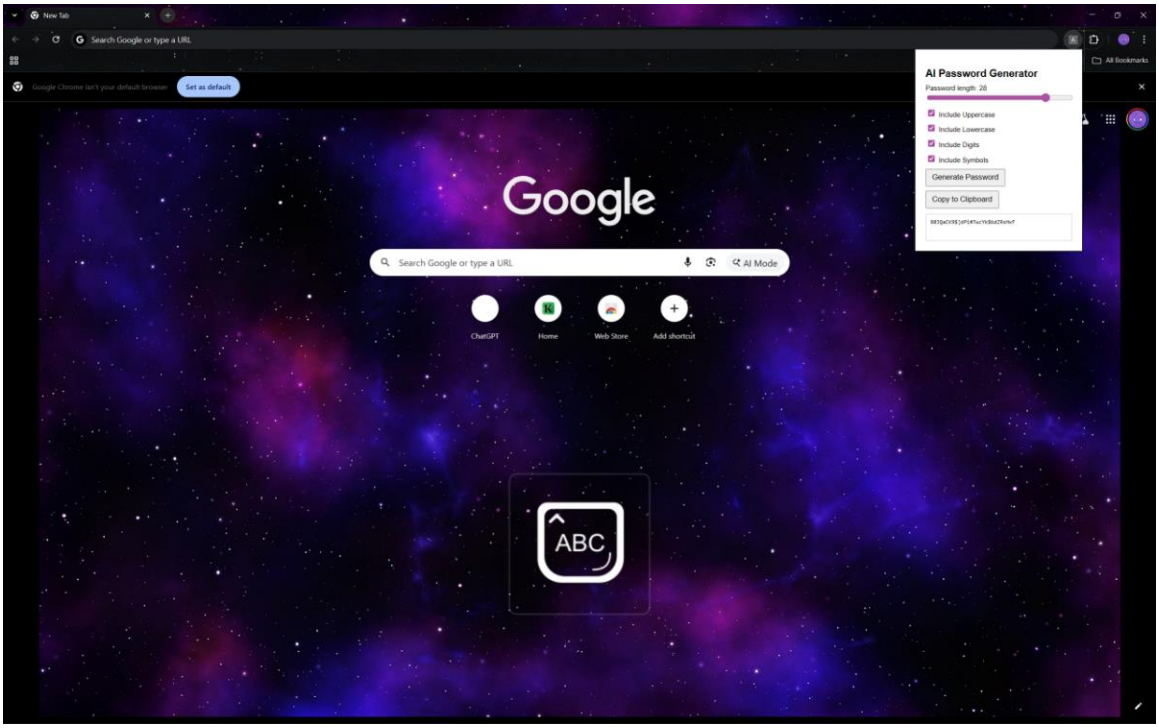
Screen Shots

1. Phishing detection





2. Password Generator

3. 

CONCLUSION

The project successfully delivers an AI-driven phishing detector and a user-friendly password generator extension. Both components enhance cybersecurity posture and user convenience.